



Opis przedmiotu zamówienia (OPZ) na dostarczenie rozwiązań oraz fizycznego sprzętu dla wdrożenia uwierzytelniania wieloskładnikowego

Przedmiotem zamówienia jest dostarczenie rozwiązań oraz fizycznego sprzętu niezbędnego do wdrożenia uwierzytelniania wieloskładnikowego.

Lp.	Nazwa	Liczba sztuk
1	Uwierzytelnianie wieloskładnikowe	130
2	Usługa wdrożenia i szkolenia	1



1.1 Wymagania: uwierzytelnianie wieloskładnikowe

Lp	Parametr wymagany
1	<p>Przedmiotem zamówienia jest zaprojektowanie, dostarczenie oraz wdrożenie w środowisku Zamawiającego rozwiązania umożliwiającego logowanie użytkowników przy użyciu fizycznych kluczy zgodnych z protokołem FIDO2, pełniących funkcję:</p> <ul style="list-style-type: none"> Karty inteligentnej (smartcard) w procesie logowania do stacji roboczych z systemem Windows 10/11. Dodatkowego czynnika uwierzytelniania wieloskładnikowego (MFA) oraz mechanizmu logowania w usługach chmurowych opartych o Entra ID (dawniej Azure Active Directory).
2	<p>Dostawa fizycznych kluczy, które będą posiadały wsparcie dla następujących protokołów:</p> <ul style="list-style-type: none"> WebAuthn OATH HOTP OATH TOTP U2F SmartCard (PIV) OpenPGP FIDO2 Yubico OTP
3	Jedną z wymaganych opcji dla fizycznych kluczy jest wbudowana funkcja komunikacji NFC.
4	Dostawa i wdrożenie mają obejmować zarówno konfigurację infrastruktury IT Zamawiającego (w tym integrację z istniejącą infrastrukturą PKI lub jej wdrożenie), jak i przygotowanie niezbędnej dokumentacji oraz przeprowadzenie szkoleń z obsługi nowego rozwiązania.
5	<p>Analiza infrastruktury Zamawiającego:</p> <ul style="list-style-type: none"> Przegląd stacji roboczych z systemem Windows 10/11 oraz ewentualnych różnic w wersjach systemu operacyjnego. Ocena istniejącej Infrastruktury Klucza Fizycznego – (PKI – Public Key Infrastructure - Active Directory Certificate Services), a w szczególności: <ul style="list-style-type: none"> Sposobu wydawania i zarządzania certyfikatami. Szablonów certyfikatów przeznaczonych do logowania przy użyciu smartcard. Weryfikacja zgodności obecnych rozwiązań z wymaganiami FIDO2.
6	<p>Weryfikacja posiadanych fizycznych kluczy FIDO2:</p> <ul style="list-style-type: none"> Weryfikacja kluczy FIDO2 pod kątem obsługi wymaganej funkcjonalności (m.in. algorytmy kryptograficzne, funkcje smartcard, mechanizmy MFA). Wykonawca musi zapewnić, że oferowane klucze FIDO2: <ul style="list-style-type: none"> Spełniają standard FIDO2/WebAuthn w zakresie bezpieczeństwa. Umożliwiają ustawienie kodu PIN lub użycie innej metody weryfikacji (np. biometrii) zależnie od wymagań Zamawiającego. Pozwalają na przechowywanie certyfikatu X.509 w celu działania jako karta inteligentna.
7	<p>Konfiguracja i dostosowanie środowiska:</p> <ul style="list-style-type: none"> Przygotowanie lub aktualizacja infrastruktury PKI (Active Directory Certificate Services): <ul style="list-style-type: none"> Stworzenie bądź dostosowanie szablonów certyfikatów. Ustalenie polityk wydawania i odnawiania certyfikatów dla kluczy.

Fundusze Europejskie

na Rozwój Cyfrowy

	<ul style="list-style-type: none"> Dostosowanie ustawień w lokalnej usłudze katalogowej i infrastrukturze chmurowej: <ul style="list-style-type: none"> Włączenie funkcji logowania kartą inteligentną. Konfiguracja polityk uwierzytelniania w usłudze katalogowej z uwzględnieniem FIDO2 jako metody dodatkowego składnika logowania. Implementacja wymogów odnośnie dodatkowego składnika uwierzytelniania (MFA) przy użyciu kluczy FIDO2 w usługach chmurowych. Testowanie poprawności działania na wybranych stanowiskach urządzeń końcowych w połączeniu z infrastrukturą Zamawiającego (lokalną oraz chmurową).
8	<p>Testy i weryfikacja poprawności:</p> <ul style="list-style-type: none"> Przeprowadzenie testów potwierdzających poprawne logowanie za pomocą kluczy FIDO2 na stacjach roboczych: <ul style="list-style-type: none"> Z wykorzystaniem konfiguracji typu smartcard (certyfikaty X.509). Wymuszanie użycia kluczy FIDO2 w wybranych grupach użytkowników zgodnie z politykami. Testy logowania i MFA w środowisku chmurowym: <ul style="list-style-type: none"> Weryfikacja mechanizmu w usłudze katalogowej. Sprawdzenie poprawności wdrożenia MFA w aplikacjach oraz usługach powiązanych. Zidentyfikowanie i usunięcie ewentualnych nieprawidłowości, sporządzenie raportu z testów.
9	<p>Monitorowanie i optymalizacja rozwiązania</p> <ul style="list-style-type: none"> Konfiguracja i udostępnienie narzędzi do monitorowania procesu logowania użytkowników. Regularna analiza bezpieczeństwa i wydajności rozwiązania (m.in. monitorowanie ewentualnych błędów logowania, incydentów, prób nieautoryzowanego dostępu). Dostosowanie polityk bezpieczeństwa i procesów w oparciu o zebrane wnioski, rekomendacje i opinie użytkowników.
10	<p>Wymagania techniczne:</p> <ul style="list-style-type: none"> Wykonawca zobowiązany jest do weryfikacji i zapewnienia, że zastosowane klucze Zamawiającego FIDO2 oraz ich oprogramowanie wspierają: <ul style="list-style-type: none"> Logowanie do systemów Windows 10/11 poprzez funkcję smartcard (certyfikat X.509). Logowanie do środowiska chmurowego Microsoft w ramach usługi katalogowej (uwierzytelnianie MFA). Klucze FIDO2 muszą obsługiwać mechanizmy kryptograficzne wymagane przez Zamawiającego, a w szczególności pozwalać na przechowywanie i bezpieczne używanie klucza prywatnego. Wymaga się, aby proces rejestracji kluczy w środowisku Zamawiającego był możliwie uproszczony i skalowalny.
11	<p>Wymagania organizacyjne:</p> <ul style="list-style-type: none"> Wykonawca dostarczy harmonogram wdrożenia uwzględniający kolejność i terminy poszczególnych etapów, w tym analizę wstępną, konfigurację PKI, konfigurację kluczy FIDO2 i testy. Wykonawca zapewni niezbędne zasoby ludzkie oraz wsparcie ekspertów w zakresie PKI, systemów Microsoft (Windows 10/11, Entra ID), a także w obszarze bezpieczeństwa IT.
12	<p>Bezpieczeństwo:</p> <ul style="list-style-type: none"> Rozwiązanie musi być zgodne z wewnętrznymi politykami bezpieczeństwa Zamawiającego, a także z powszechnie obowiązującymi przepisami dotyczącymi ochrony

Fundusze Europejskie

na Rozwój Cyfrowy

	<p>danych (np. RODO).</p> <ul style="list-style-type: none"> Wymagane jest uniemożliwienie dostępu do stacji roboczych bądź zasobów chmurowych przy braku fizycznego klucza i znajomości kodu PIN (lub innej weryfikacji). Zastosowana architektura musi zapewniać również ścieżkę awaryjną (np. odzyskania dostępu w razie utraty klucza FIDO2).
13	<p>Oczekiwane rezultaty:</p> <ul style="list-style-type: none"> Wdrożone i skonfigurowane fizyczne klucze bezpieczeństwa posiadane przez Zamawiającego dla wybranych użytkowników lub grup użytkowników zgodnie z polityką Zamawiającego. Integracja z chmurową usługą katalogową umożliwiającą korzystanie z kluczy FIDO2 jako jednego ze składników MFA. Kompleksowe szkolenia i dokumentacja ułatwiający użytkownikom korzystanie z nowego sposobu logowania, a działowi IT – zarządzanie i utrzymanie rozwiązania. Raport powdrożeniowy zawierający opis przeprowadzonych testów, ewentualnych problemów oraz rekomendacje dalszych działań optymalizacyjnych. Klucze muszą zostać wykonane z indywidualną grafiką
14	Wymagana jest analiza obecnych rozwiązań Zamawiającego, dostosowanie zaproponowanych rozwiązań konfiguracji po wcześniejszym obopólnym uzgodnieniu i zaakceptowaniu przez strony.
15	Zaproponowane rozwiązanie musi być integralne z funkcjonalnościami zewnętrznego oprogramowania ESET Secure Authentication.
16	Gwarancja udzielona przez Wykonawcę na fizyczny sprzęt musi wynosić nie mniej niż 36 miesięcy od daty dostawy.
17	Instruktaż powdrożeniowy dla Administratorów systemu: min. 8h w terminach wcześniej ustalonych i potwierdzonych przez Zamawiającego.